12

#23/Appeal Brief
Ellis
5/26/04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of:	)Attorney Docket No.: E-731
Linda V. Gravell et al.	)Group Art Unit: 3621
Serial No.: 09/242,210	)Examiner: C. Scherr
Filed: Nov. 4, 1999	)Date: May 18, 2004

Confirmation No.: 9775

Title: VIRTUAL POSTAGE METERING SYSTEM

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF ON APPEAL

Sir:

This is an appeal pursuant to 35 U.S.C. § 134 and 37 C.F.R. §§ 1.191 et seq. from the final rejection of claims 1 and 9-18 of the above-identified application mailed November 24, 2003. The fee for submitting this Brief is $330.00 (37 C.F.R. § 1.17(c)). Please charge Deposit Account No. **16-1885** in the amount of $330.00 to cover these fees. The Commissioner is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. **16-1885**. The Notice of Appeal was received by the U.S. Patent and Trademark Office on March 22, 2004. Enclosed with this original are two copies of this brief.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on May 18, 2004
Date of Deposit

Signature

Brian A. Lemm
Name of Registered Rep.

May 18, 2004
Date

I. Real Party in Interest

The real party in interest in this appeal is Pitney Bowes Inc., a Delaware corporation, the assignee of this application.

II. Related Appeals and Interferences

There are no appeals or interferences known to Appellants, their legal representative, or the assignee that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. Status of Claims

Claim 1 stands rejected under 35 U.S.C. § 102(e) as being anticipated by Kara (U.S. Patent No. 5,822,739). Claims 9-18 stand rejected under 35 U.S.C. § 102(e) as being anticipated by, or, in the alternative, under 35 U.S.C. § 103(a) as obvious over, Whitehouse (U.S. Patent No. 6,005,945).

IV. Status of Amendments

There are no amendments to the claims filed subsequently to the final rejection of November 24, 2003. Therefore, the claims as set forth in Appendix A to this brief are those as set forth before the final rejection.

V. Summary of Invention

Appellants' invention relates to a virtual postage metering system in which a host of personal computers (PC) are coupled to a server located at a data center. The host PC's do not have any Postage Storage Devices (PSD) coupled thereto; instead, all PSD functions are performed at the data center. The PSD is a secure processor-based accounting device that dispenses and accounts for postal value stored therein. The host PCs must connect with the data center to process transactions such as postage dispensing, meter registration or meter refills. Transactions are requested by the host PC and sent to the data center for remote processing. The transactions are processed centrally at the data center and the results are returned to the host PC. Accounting for funds and transaction processing are centralized at the data center. (Specification, page 4).

Although the data center may be a secure facility, there remain certain inherent security issues since the accounting and token generation functions do not occur in a secure device local to the postage meter. For example, data stored at the data center is accessible to data center personnel and, therefore, at a minimum, subject to at least inadvertent modification by such personnel. Any unauthorized changes to the user and meter data stored at the data center compromises the integrity of the virtual postage metering system. (Specification, page 5). The present invention alleviates these types of security issues by providing a virtual postage metering system in which the transaction records are signed with a digital signature and the signed transaction records are stored at the data center. Thus, if the information contained within the transaction record has been altered, the digital signature will not verify, thereby indicating that the information has been altered. Thus, the signed record is unalterable and the signature cannot be repudiated.

Additional features of the invention are discussed below in the Argument section of this Brief.

VI. Issues

A. Whether the subject matter defined in claim 1 is anticipated by Kara.

B. Whether the subject matter defined in claims 9-18 is anticipated by or rendered obvious by Whitehouse.

VII. Grouping of Claims

Claims 1 and 9-18 are grouped in the following groups:

Group I - Claim 1.

Group II - Claims 9-18.

None of the claims in the different Groups stand or fall together. In Group II, claims 9 and 12-14 stand or fall together, claims 10 and 11 stand or fall together, claims 14, 17 and 18 stand or fall together, and claims 15 and 16 stand or fall together. The reasons why the Appellants believe the remaining claims to be separately patentable are set forth in the Argument section of this Brief.

VIII. Argument

As Appellants discuss in detail below, the final rejection of claims 1 and 9-18 is devoid of any factual or legal premise that supports the position of unpatentability. It is respectfully submitted that the rejection does not even meet the threshold burden of presenting a prima facie case of unpatentability. For this reason alone, Appellants are entitled to grant of a patent. In re Oetiker, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992).

A. The subject matter defined by claim 1 is not anticipated by Kara.

Claim 1 is directed to a method for evidencing postage that comprises "generating a digital token . . . including encrypted information for the mailpiece . . . creating a transaction record . . . including the digital token and the postal information; signing the transaction record" and "storing the transaction record in a database at the data center."

The Final Rejection contends that Kara discloses signing a transaction record and storing the transaction record in a database at Col. 14, lines 12-36 and Col. 4, lines 37-50. Appellants respectfully disagree. Col. 14, lines 12-38 of Kara state:

> Upon determination of proper funding, the Meter program increments a record of the amount of postage credit transmitted for later compensation to the Postal Authority. Alternatively, the Meter program deducts the amount of postage to be used by the postage indicia from a postage credit available at PC 10 (step 306). The Meter program may itself be provided with postage credit through such means as authorization by an official postal service, direct connection to a postal service office, or portable electronic postage credit. The details of the provision of postage credit to the Meter program is not shown, but may be, for example, the system shown in above referenced and incorporated U.S. Pat. No. 5,510,992.
>
> The Meter program may check the destination address included in the demand to verify that it is a proper address if desired. Address checking is accomplished by comparing the destination address to a database of addresses stored, for example, on disk drive 13 within PC 10.
>
> The Meter program utilizes information contained within the demand to generate a data packet representing the desired postage indicia (step 307). The data packet includes information required of a valid postage indicia by a postal service. Such information may include the date of posting, the amount of the postage, a unique transaction identifier, and identification of the metering device. The information may also include data to be printed with the postage indicia, such as the sender's return address, at the user's preference.

Col. 4, lines 37-50 of Kara state:

> In the preferred embodiment, the Demand program provides security at the demand site to prevent unauthorized utilization of the postage metering system. The appropriate level of security for any installation of the Demand program can be chosen by a principal at each location, thereby providing a distributed security system. Distributed security provides the ability for individual users of the postage metering system to select a level of security appropriate to prevent postal theft in their environment. Such distributed security does not increase the risk of postage loss at the remote meter as, regardless of the level of security chosen at the demand site, verification is performed by the Meter program to ensure each demand is valid and properly funded.

Note first that there is nothing in either of these passages that relates to signing a transaction record and storing the transaction record in a database as is recited in claim 1, nor has the Final Rejection provided any specific reference to where these features are allegedly disclosed. The Final Rejection contends that a "unique transaction identifier" is equivalent to signing a transaction. This is simply not true. The unique transaction identifier in Kara is merely an identifier of the transaction, such as, for example, a serial number or the like. Thus, the information contained within the transaction record can be altered or changed and the "unique transaction identifier" can remain the same. Thus, there is no way of determining if the information contained within the transaction record has been altered. The "unique transaction identifier" does not provide any type of protection against such alteration, nor does it provide any type of authentication of the author. A digital signature, in contrast, authenticates and protects the integrity of the information in the transaction record. If the information contained within the transaction record has been altered, the digital signature will not verify, thereby indicating that the information has been altered. Thus, the signed record is unalterable and the signature cannot be repudiated. These attributes are not present in a "unique transaction identifier," as there is no resemblance between a unique transaction identifier and a digital signature.

Col. 4, lines 37-50, of Kara are directed to providing security at the demand site to prevent unauthorized use of the postage metering system. In Kara, a demand program is stored on first processor-based system (PC) located within a business' office or an individual's home. The demand program accepts information from a user and makes a demand for postage to a remote postage meter, itself a second processor-based system in the form of a PC, that is located at a postage provider's office or other central source. The second PC stores a meter program that verifies postage demands and electronically transmits the desired postage indicia to the first PC in the form of a data packet. (Col. 3, line 55 to Col. 4, line 4). Thus, the security at the demand site is designed to limit access to the demand program. For example, as illustrated in Fig. 2 of Kara, at step 201 upon activation of the demand program, the user is asked for, and the process accepts, a user password. At step 202, the demand program determines if the accepted password is valid. If the password is not valid, the process returns to step 201, thus preventing unauthorized access to postage. (Col. 7, lines 47-55). This is in no way related to creating a transaction record, signing the transaction record, and storing the transaction record in a database at a data center as is recited in claim 1.

Furthermore, in Kara, a meter program is used to generate a data packet that is a digital representation or image of the postage indicia to be ultimately printed by the demanding site. The data packet includes information required of a valid postage indicia by a postal service. (Col. 14, lines 30-41). Thus, the data packet is sent to the demanding site for use in printing the indicia. Specifically, at step 308 of Fig. 3, the data packet generated from the received demand is transmitted via the data communications link to the demand site. (Col. 15, lines 1-3). There is no disclosure, teaching or suggestion in Kara of creating a transaction record, signing the transaction record, and storing the signed transaction record in a database at the data center as is recited in claim 1.

For at least the above reasons, Appellants respectfully submit that the final rejection as to claim 1 is in error and should be reversed.

B. The subject matter defined in claims 9-18 is not anticipated by nor rendered obvious by Whitehouse.

Claim 9 is directed to a system for dispensing postage that includes a data center, the data center comprising a "storage device," a "first cryptographic module" that includes a "first key to decrypt a user authentication key included in the user account, the user authentication key being used to authenticate the user; and a second cryptographic module . . . including a second key to decrypt a token key included the meter account, the token key used to generate a digital token, the second cryptographic module further including a third key used to sign a transaction record associated with generating the digital token, the signed transaction record being stored in the storage device."

The Final Rejection contends that Col. 8, lines 37-41, and Col. 14, lines 26-48, of Whitehouse disclose signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center. Appellants respectfully disagree. Col. 8, lines 30-53, of Whitehouse state:

> Local memory 154, which will typically include both random access memory and non-volatile disk storage, preferably stores a set of postage dispensing procedures 160, including:
>
> a postage indicium request validation procedure 161 for validating requests from end user computers for postal indicia;
>
> message encryption and decryption procedures 162;

> encryption keys 164 needed to generate the digital signatures in postal indicia, and keys for secure communications with the postal authority computer system 180;
>
> a ZIP+4 or ZIP+4+2 procedure 166 for generating a ZIP+4 or ZIP+4+2 value for each destination address specified in a postage request message received from any of the customer PCS;
>
> an indicium generation procedure 168 for generating a sequence of bits representing a postage indicia corresponding to a destination address specified by a customer PC, including a procedure for digitally signing each postage indicium; and
>
> a communication procedure 170 for handling communications with the customer PCS 104.

While the above passage discusses the use of encryption keys to generate digital signatures in postage indicia, there is no disclosure, teaching or suggestion of signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9.

Col. 14, lines 25-56, of Whitehouse state:

> The integrity of the balance update transaction depends upon a coordinated encryption/decryption between the funding entity (typically a postage meter vendor) and the end user. For conventional electronic meters, the encryption is based on a complex formula involving the internal meter ID, the amount of postage required, the descending and ascending registers in the meter, the date and other variables. Security in this transaction is absolutely critical because the dollar amount is frequently substantial, and because the funds transferred are more or less "unmarked". The reference to "unmarked" will be better explained in the next paragraph.
>
> The present invention completely abandons the concept of a locally maintained postage balance. Instead the official balance for any given user is maintained at the centralized secure computer. The balance may be increased at any time by the user through any number of secure means (e.g., a check taken to a local post office, funds mailed, or credit card transactions via the Web). All of these postage increase transactions are handled by the central secure site where standard payment verification techniques can be applied before the balance is actually updated.
>
> FIG. 6 underscores another aspect of the security offered by this invention. When

> funds are drawn against a license (meter) account's balance, contact must be made with the central secure computer and all relevant information about the mail piece must be conveyed for this transaction to be successfully processed. The information returned amalgamates the proper amount of postage and the delivery information for this particular mail piece--and it is this information that is used to create a two-dimensional IBIP barcode.

While the above passage discusses the need for security in the transaction between the postage meter vendor and the end user, there is no disclosure, teaching or suggestion of signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9.

Whitehouse is directed to a system for the electronic distribution of postage wherein all secure processing required for generating postal indicia is performed at secure central computers, not at end user computers, thereby removing the need for specialized secure computational equipment at end user sites. In Whitehouse, a typical secure central computer includes a data processor and a database of information concerning user accounts of users authorized to request postal indicia from the secure central computer. A request validation procedure authenticates received postage request with respect to the user account information in the database. A postal indicia creation procedure applies a secret encryption key to information in each authenticated postage request so as to generate a digital signature and combines the information in each authenticated postage request with the corresponding generated digital signature so as to generate a digital postage indicium in accordance with a predefined postage indicium data format. A communication procedure securely transmits the generated digital postage indicium to the requesting end user computer. (Col. 6, lines 20-45).

In Whitehouse, the data stored by the secure central computer 102 in its customer database for each meter/user account includes various information related to the account. In addition, for each meter or account, at least two child transaction tables are maintained in the transaction database 174. The first is a record of postage purchases, and the second transaction table records each postage indicium dispensing event. Whitehouse further indicates that storing data on the central computer offers very distinct advantages over conventional meters or the

PSD, since the meter balances are stored on computer media rather than secure non-volatile meter registers. (Col. 10, line 45 to Col. 11, line 56).

Thus, although Whitehouse may store significant amounts of data at the central computer, there is no disclosure, teaching or suggestion in Whitehouse of signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9. In fact, Appellants respectfully submit that Whitehouse teaches away from the present invention, since as noted above Whitehouse indicates that storing data on the central computer offers very distinct advantages over conventional meters or the PSD, since the meter balances are stored on computer media rather than secure non-volatile meter registers. Thus, the data stored in Whitehouse is not secured as is done in the present invention by signing the transaction records before storing them. Thus, there is no disclosure, teaching or suggestion in Whitehouse of signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9.

Although Whitehouse discusses the use of a digital signature, this signature is added to the other parts of the postage indicium and a message, including data representing the postage indicium with the digital signature, is encrypted and then the resulting message is transmitted to the requesting user. (Col. 13, line 15-50). This is not the same as signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9.

"Determination of obviousness can not be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention. There must be a teaching or suggestion within the prior art, or within the general knowledge of a person of ordinary skill in the field of the invention, to look to particular sources of information, to select particular elements, and to combine them in a way they were combined by the inventor." ATD Corp. v. Lydall, Inc., 159 F.3d 534, 545 (Fed. Cir. 1998) (emphasis added). No such suggestion or motivation has been provided by the Final Rejection. The fact that the present invention was made by the Applicants does not make the present invention obvious; that suggestion or teaching must come from the prior art. See C.R. Bard, Inc. v. M3 Systems, Inc., 157 F.3d 1340, 1352 (Fed. Cir. 1998). See, e.g., Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051-1052 (Fed. Cir. 1988) (it is impermissible to reconstruct the claimed invention from selected pieces of prior art absent some suggestion, teaching, or motivation in the prior art to do so.)

Without using the present claims as a road map, it would not have been obvious to make the multiple, selective modifications needed to arrive at the claimed invention from this reference. The rejection uses impermissible hindsight to reconstruct the present invention from this reference. See Ex parte Clapp, 227 U.S.P.Q. 972,973 (Bd. App. 1985) (requiring "convincing line of reasoning" to support an obviousness determination).

For at least the above reasons, Appellants respectfully submit that the final rejection as to claim 9 is in error and should be reversed. Claims 10-13 are dependent upon claim 9 and therefore the final rejection with respect to these claims should also be reversed.

Claim 10 is patentable, however, separate and apart from its dependency on claim 9 in that it includes novel limitations and a unique combination that would not have been obvious at the time of the invention. Specifically, claim 10 includes the further limitation of a third cryptographic module coupled to the storage device, the third cryptographic module including a fourth key used to sign a user transaction record, the user transaction record being stored in the storage device. There is no disclosure, teaching or suggestion in Whitehouse of a third cryptographic module that includes a fourth key used to sign a user transaction record that is stored in the storage device as is recited in claim 10.

For at least the above reasons, Appellants respectfully submit that the final rejection as to claim 10 is in error and should be reversed. Claim 11 is dependent upon claim 10 and therefore the final rejection with respect to this claim should also be reversed.

Claim 14 is directed to a method for performing a postage evidencing transaction that comprises "receiving at a data center a request for postage evidencing from a remote computer, the request including information related to a mailer; providing a first record associated with the mailer stored in the data center to a first cryptographic module at the data center, the first cryptographic module using a first key to decrypt a user authentication key included in the first record, the user authentication key being used to authenticate the mailer; providing a second record to a second cryptographic module at the data center, the second cryptographic module using a second key to decrypt a token key included in the second record, the second cryptographic module using the token key to generate a digital token, the second cryptographic module further generating a transaction record associated with generating the digital token; using a third key to sign the transaction record; storing the signed transaction record at the data center; and sending the digital token to the remote computer to be included as postage evidence on a mailpiece."

As noted above with respect to claim 9, there is no disclosure, teaching or suggestion in Whitehouse of signing a transaction record associated with generating the digital token and storing the signed transaction record at the data center as is recited in claim 14.

For at least the above reasons, Appellants respectfully submit that the final rejection as to claim 14 is in error and should be reversed. Claims 15-18 are dependent upon claim 14 and therefore the final rejection with respect to these claims should also be reversed.

Claim 15 is also patentable, separate and apart from its dependency on claim 14, in that it includes novel limitations and a unique combination that would not have been obvious at the time of the invention. Specifically, claim 15 includes the further limitations of "generating a user transaction record each time a user accesses the data center; signing the user transaction record with a fourth key; and storing the signed user transaction record at the data center." There is no disclosure, teaching or suggestion in Whitehouse of using a fourth key to sign a user transaction record that is stored at the data center as is recited in claim 15.

For at least the above reasons, Appellants respectfully submit that the final rejection as to claim 15 is in error and should be reversed. Claim 16 is dependent upon claim 15 and therefore the final rejection with respect to this claim should also be reversed.

IX. Conclusion

In Conclusion, Appellants respectfully submit that the final rejection of claims 1 and 9-18 is in error for at least the reasons given above and should, therefore, be reversed.

Respectfully submitted,

Brian A. Lemm
Reg. No. 43,748
Attorney for the Appellants
Telephone (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, Connecticut 06484-8000

APPENDIX A

1. A method for evidencing postage on a mailpiece comprising the steps of:

receiving at a data center postal information relating to a mailpiece, said postal information including recipient address information for the mailpiece;

generating a digital token for the mailpiece, said digital token including encrypted information for the mailpiece based on said recipient address information;

creating a transaction record, said transaction record including the digital token and the postal information;

signing the transaction record;

storing the transaction record in a database at the data center; and

performing value added services using the transaction record.

9. A system for dispensing postage value comprising:

a data center communicatively coupled to a remote processor via a network, a user initiating a request to the data center via the remote processor to dispense postage value to be printed by a printer coupled to the remote processor, the data center comprising:

a storage device to store data records, the data records including a user account and a meter account associated with the user;

a first cryptographic module coupled to the storage device, the first cryptographic module including a first key to decrypt a user authentication key included in the user account, the user authentication key being used to authenticate the user; and

a second cryptographic module coupled to the storage device, the second cryptographic module including a second key to decrypt a token key included in the meter account, the token key used to generate a digital token, the second cryptographic module further including a third key used to sign a transaction record associated with generating the digital token, the signed transaction record being stored in the storage device;

wherein the data center sends the digital token to the remote processor via the network.

10. The system according to claim 9, wherein the data center further comprises:

a third cryptographic module coupled to the storage device, the third cryptographic module including a fourth key used to sign a user transaction record, the user transaction record being stored in the storage device.

11. The system according to claim 10, wherein the first, second , third and fourth keys are identical.

12. The system according to claim 9, wherein the data center further comprises:

a key management system to manage the first, second and third keys.

13. The system according to claim 9, wherein the network is the Internet.

14. A method for performing a postage evidencing transaction comprising the steps of:

receiving at a data center a request for postage evidencing from a remote computer, the request including information related to a mailer;

providing a first record associated with the mailer stored in the data center to a first cryptographic module at the data center, the first cryptographic module using a first key to decrypt a user authentication key included in the first record, the user authentication key being used to authenticate the mailer;

providing a second record to a second cryptographic module at the data center, the second cryptographic module using a second key to decrypt a token key included in the second record, the second cryptographic module using the token key to generate a digital token, the second cryptographic module further generating a transaction record associated with generating the digital token;

using a third key to sign the transaction record;

storing the signed transaction record at the data center; and

sending the digital token to the remote computer to be included as postage evidence on a mailpiece.

15. The method according to claim 14, further comprising:

generating a user transaction record each time a user accesses the data center;

signing the user transaction record with a fourth key; and

storing the signed user transaction record at the data center.

16. The method according to claim 15, further comprising:

verifying the user transaction record when a next transaction is requested.

17. The method according to claim 14, further comprising:

providing value added services to the mailer, the value-added service including at least one of on-line rating, special mail services, address cleansing and postal coding services.

18. The method according to claim 14, further comprising:

providing on-line tracking of all postal transaction processed by the data center.